

SP 800-90B Non-Proprietary Public Use Document
Junos OS™ 25.2 Kernel CPU Time Jitter RNG Entropy
Source version 3.4.1
Document version 1.0

Juniper Networks, Inc.
1133 Innovations Way
Sunnyvale, CA 94089
United States

Revision History

Version	Change
2026-07-20	Initial draft

Table of Contents

Description 4
Security Boundary 4
Operating Conditions 4
Configuration Settings 5
Physical Security Mechanisms 6
Conceptual Interfaces 6
Min-Entropy Rate 6
Health Tests 7
Maintenance 7
User Verification 7

Juniper Business Use Only

Description

This Junos OS™ 25.2 Kernel CPU Time Jitter RNG Entropy Source is a non-physical (NP), non-IID source composed of the jitterentropy-library v3.4.1 embedded within the Junos OS kernel firmware.

CPU Jitter RNG makes no IID claim and thus meets all the requirements for a non-IID entropy source. The operational environments tested are listed in Table 1 below.

The entropy source was assessed against NIST SP 800-90B (2018) and FIPS 140-3 IG (April 16th, 2026) sections D.J (November 5th, 2021), D.K (April 16th, 2026) and D.O (May 4th, 2021).

Security Boundary

The security boundary of the entropy source coincides with the FIPS 140-3 cryptographic boundary of the modules listed in Table 1, which is the outer edge of the chassis. These cryptographic modules consist of production grade components enclosed in production grade removable metal enclosures as described in their respective FIPS Security Policies.

The entropy source architecture is as follows:

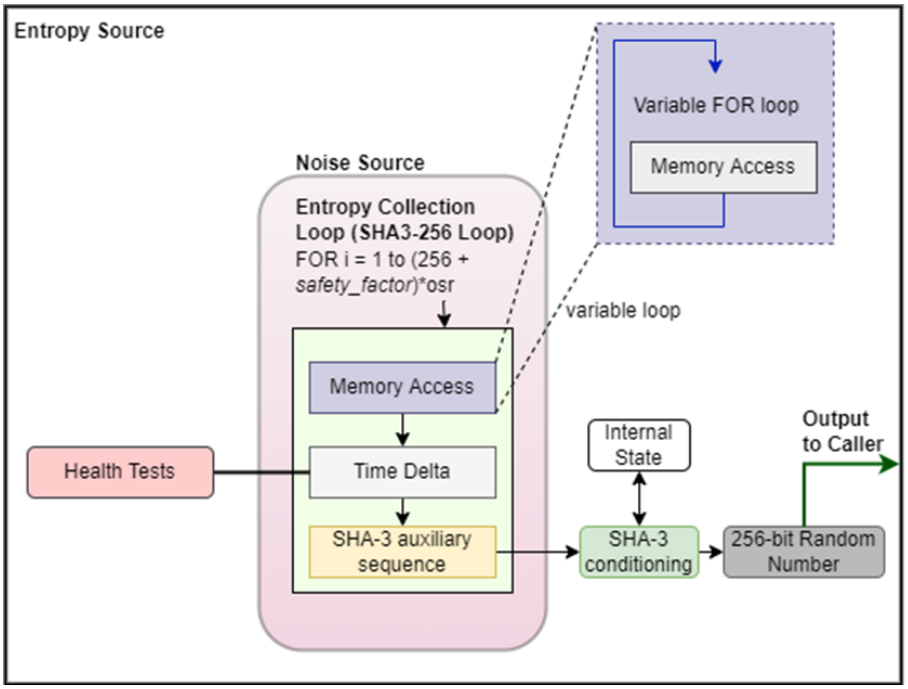


Figure 1. CPU Jitter Entropy Source Diagram

Operating Conditions

The operating conditions are inherited from the operational environment in which the entropy source executes, as shown in Table 1 below:

Product	Junos OS Version	CPU	Cache	Temperature	Humidity
EX4100-H switch series	25.2R2	ARM® Cortex® A72	L1: 48 KB instruction + 32 KB data L2: 1 MB combined L3: none	-40° F (-40° C) to 140° F (60° C)	5% to 95%, non-condensing. Up to 15,000 ft altitude.
EX4100 switch series	25.2R2	ARM® Cortex® A72	L1: 48 KB instruction + 32 KB data L2: 1 MB combined L3: none	32° F (0° C) to 113° F (45° C)	5% to 95%, non-condensing. Up to 5,000 ft altitude.
EX4000 switch series	25.2R2	ARM® Cortex® A55	L1: 32 KB instruction + 32 KB data L2: 64K combined L3: 1 MB	32° F (0° C) to 104° F (40° C)	5% to 90%, non-condensing

Table 1. Operating Environment and Conditions

Configuration Settings

The entropy relevant parameters are listed in Table 2 *CPU Jitter Compilation Configuration Parameters*, Table 3 *CPU Jitter Runtime Configuration Flags* and Table 4 *Platform-Specific Parameters*.

Parameter	Default Value
JENT_CONF_DISABLE_LOOP_SHUFFLE	Defined
JENT_HEALTH_LAG_PREDICTOR	Defined
JENT_RANDOM_MEMACCESS	Defined
ENTROPY_SAFETY_FACTOR	64
JENT_MIN_OSR	3
JENT_MEMORY_SIZE	2^{20}
JENT_MEMORY_BITS	20
JENT_MEMORY_ACCESSLOOPS	128
JENT_CONF_ENABLE_INTERNAL_TIMER	Not Defined
JENT_APT_WINDOW_SIZE	512
JENT_LAG_WINDOW_SIZE	2^{17}
JENT_LAG_HISTORY_SIZE	8
JENT_POWERUP_TESTLOOPCOUNT	1024
CLEARCACHE	100
MIN_HASH_LOOP	0

Parameter	Default Value
MIN_ACC_LOOP_BIT	0

Table 2. CPU Jitter Compilation Configuration Parameters

Parameter	Status	Implemented Value	Argument Name	Meaning
JENT_DISABLE_MEMORY_ACCESS	Prohibited	Not in use	flags	Disable the memory access timing.
JENT_FORCE_INTERNAL_TIMER	Prohibited	Not in use	flags	Force use of pthreads-based internal timer, rather than the underlying hardware timer.
JENT_DISABLE_INTERNAL_TIMER	Allowed	Not in use	flags	Prevent the use of the pthreads-based internal timer. Since JENT_CONF_ENABLE_INTERNAL_TIMER is not defined, it is not possible to use the internal timer.
JENT_FORCE_FIPS	Required	Always set	flags	Force fips_enabled to be set (enabling health test reporting and use of the safety factor).
JENT_MAX_MEMSIZE_*	Prohibited	Not in use	flags	Allows for run-time selection of the memory region size.

Table 3. CPU Jitter Runtime Configuration Flags

Platform	Memory Size	OSR
EX4100-H	8 GB	3
EX4100	8 GB	3
EX4000	4 GB	3

Table 4. Platform-Specific Parameters

Physical Security Mechanisms

Not applicable, as the entropy source is restricted to the vendor.

Conceptual Interfaces

The GetEntropy interface, corresponding to the *jent_read_entropy* API, is called by the Junos OS kernel DRBG for seeding and reseeding purposes.

Min-Entropy Rate

The entropy source provides 256 bits of entropy per 256-bit conditioned output block.

Health Tests

The entropy source implements the following health tests:

- Stuck Test
- Repetition Count Test
- Adaptive Proportion Test
- Lag Predictor Test

In conformance with NIST SP 800-90B, these health tests are performed in three circumstances:

- Start-up Tests: The entropy source performs start-up health tests on 1024 samples. If any of the above tests fail, the entropy source halts and does not produce any further output. The entropy source does not output any data until both the requisite number of samples has been collected and the start-up health tests have passed.
- Continuous Tests: The entropy source performs continuous health tests during operation. If any of the tests fail, the error is logged and the entropy source halts.
- On-Demand Tests: The entropy source will perform on-demand tests when the cryptographic module is restarted.

Maintenance

This module does not require any maintenance.

User Verification

The module performs both start-up and continuous health tests as per NIST SP 800-90B. The start-up health tests may be triggered by restarting the cryptographic module in which it is contained. No explicit user verification of the health of the entropy source is necessary, as the modules that contain the source will not complete the boot process if the health tests fail.

To identify the running Junos OS version, and hence the version of the entropy source in use, issue the *show version* command from the Junos OS command line interface. This also identifies the specific product in use.